Kim Gunnink MA

Ken je **klassiekers**

Hoe verhoog je als organisatie je cyberweerbaarheid? Tips voor de auditor.

De werknemers op de redactie van TV5 Monde zagen het voor hun ogen gebeuren: de Twitteraccounts werden overgenomen, vervolgens de Facebookpagina en daarna de andere social-mediapagina's van het bedrijf. Op hetzelfde moment werden de tv-uitzendingen verstoord. De oorzaak? In de avond van 8 april 2015 werd het Franse televisiestation gehackt. Ruim 18 uur lang waren de websites van de nieuwssite onbereikbaar en gingen de tv-zenders op zwart. De directeur van het tv-station stelde dat er sprake moest zijn van een 'buitengewoon zware cyberaanval', want 'we hebben zeer sterke firewalls die we recent hebben laten controleren en toen waren ze in orde'.

Overmacht of niet?

Veel mensen voelen mee met deze directeur. Wanneer een organisatie sterke preventieve IT-maatregelen treft om aanvallers buiten de deur te houden, moet er sprake zijn van overmacht – althans, zo is de gedachte. De directeur maakt echter twee klassieke fouten met zijn uitspraak. Preventieve maatregelen – zoals een recent geüpdatete firewall – kunnen niet uitsluiten dat cyberaanvallers een organisatie schade berokkenen. Detectiemethoden, een goede respons en doordachte herstelmaatregelen zijn een noodzakelijke aanvulling. Ook zijn maatregelen voor IT-systemen of bij het ICT-departement onvoldoende om te garanderen dat een organisatie weerbaar is tegen cyberdreigingen en over de veerkracht beschikt om te herstellen na een geslaagde aanval. Cyber is meer dan alleen IT: mensen, processen en communicatie moeten ook onderdeel zijn van de cyberweerbaarheidsmaatregelen die een organisatie treft. Door als auditor bewustzijn te creëren op deze twee punten draag je bij aan een integraal cyberweerbaarheidsbeleid binnen de organisatie waarvoor je werkt.

Een cyclus van preventie, detectie, respons en herstel

Het nemen van preventieve maatregelen stond tot in de jaren negentig gelijk aan veilig zijn. Rond de millenniumwisseling realiseerde men zich echter dat ongeacht hoe sterk de preventieve maatregelen zijn, iedere organisatie op een zeker moment gehackt wordt. En als dat gebeurt, kun je er maar beter klaar voor zijn. Dus kwam detectie in zwang: hoe eerder een aanvaller wordt opgemerkt hoe minder schade hij kan toebrengen. Inmiddels leeft het besef dat preventie en detectie ook niet zaligmakend zijn. Er is immers altijd sprake van (enige) schade, ongeacht het tijdsbestek waarbinnen een succesvolle aanval ontdekt wordt. Dat betekent dat er respons- en herstelmaatregelen klaar moeten liggen om effectief met de gevolgen van een geslaagde aanval om te gaan. Om het herstel te voltooien is het belangrijk dat de situatie wordt geëvalueerd en dat de lessen die daaruit voortkomen, worden gebruikt om de gehele keten met veerkrachtvergrotende maatregelen te versterken. Dit kan bijvoorbeeld door het aanpassen van trainingen voor medewerkers, het updaten van detectiesystemen en het aanscherpen van herstelprocedures.

Cyber is meer dan IT

Auditors spelen een belangrijke rol bij het helpen voorkomen dat hun organisatie in dezelfde valkuil trapt als de directie van TV5 Monde. Uitdragen dat een organisatie voor haar eigen veiligheid bredere maatregelen moet treffen dan het sluiten van de poorten, is slechts een eerste stap. Cyber is immers veel meer dan IT alleen. Om de cyberweerbaarheid en de veerkracht van een organisatie te vergroten moeten er maatregelen getroffen worden in vier categorieën. Een daarvan is zeker IT, maar minstens zo belangrijk zijn mensen, processen en communicatie. Auditors kunnen stimuleren dat er in hun organisatie ook in deze laatste drie categorieën op een bewuste manier met cyberrisico's wordt omgegaan.

Menselijk vlak

Op het menselijke vlak zijn cultuur en bewustzijn bepalende factoren als het gaat om cyberweerbaarheid. Zo is het van groot belang dat het bestuur en senior management van een

organisatie cyberrisico's begrijpen, het belang van informatiebeveiliging erkennen en de relevantie ervan uitdragen naar de medewerkers. Dit uit zich onder meer in regelmatig terugkerende, gerichte bewustwordingstrainingen voor medewerkers op alle niveaus, inclusief het hoger management.
Bewustzijn van cyberrisico's onder de eigen medewerkers vergroot niet alleen de bescherming van de organisatie doordat mensen bijvoorbeeld minder snel in een phishing mailtje trappen, maar ook omdat het de tijd verkort tot een aanval ontdekt wordt. Het is daarbij belangrijk dat er een positieve meldcultuur bestaat in de organisatie: mensen moeten aangemoedigd worden om melding te maken van een mogelijk risico en moeten niet bang hoeven te zijn voor een reprimande omdat ze per ongeluk een verkeerde bijlage hebben geopend.

'Security by design'
Bewust omgaan met cyberrisico's in organisatieprocessen verkleint de kans op een geslaagde aanval en kan tevens de impact van een aanval beperken als deze wél slaagt: security by design. Intern kun je daarbij denken aan het inrichten van een proces waarbij alle hard- en software en de netwerkinstellingen van een organisatie periodiek grondig getest worden aan de hand van relevante veiligheidsstandaards. Ook kan ervoor worden gezorgd dat het aanvalsoppervlak zo klein mogelijk is: beperk het aantal punten dat een aanvaller kan gebruiken om de systemen binnen te dringen en waarlangs informatie naar buiten kan worden gesmokkeld. Het dusdanig beperken van systeemtoegangsrechten dat alleen degenen voor wie vanuit operationeel oogpunt systeemtoegang noodzakelijk is, is hier een voorbeeld van.
Security by design heeft ook betrekking op relaties met ketenpartners. Het komt namelijk niet zelden voor dat cyberaanvallers een derde partij als kruiwagen gebruiken om binnen te dringen bij hun uiteindelijke doelwit. Dit kan ver gaan: een notoir voorbeeld is de hack van de Amerikaanse supermarktketen Target eind 2013, waarbij de aanvallers nota bene via de aircoleverancier van de keten door wisten te dringen tot de point-of-salesystemen en vandaar uit de gegevens van meer dan 40 miljoen credit- en debitkaartgebruikers wisten te stelen.
Rekening houden met cyberrisico's tijdens bijvoorbeeld de onderhandelingen over servicecontracten met een derde partij maakt duidelijk waar verantwoordelijkheden en aansprakelijkheden liggen en vergemakkelijkt de communicatie als er sprake is van een aanval.

Communicatie
Ook vanuit communicatieoogpunt moet een organisatie rekening houden met cyberrisico's. Als er bekend is wat er op welk moment aan wie gecommuniceerd moet worden wanneer een cyberaanval ontdekt is, kan de schade ingedamd worden. Informatie delen met zowel de eigen medewerkers als externe belanghebbenden zoals relevante autoriteiten, klanten, ketenpartners en media is cruciaal. Door deze betrokkenen te informeren, kunnen verdere verspreiding van de aanval, speculatie over wat er gaande is en eventuele paniekreacties onder klanten beperkt worden.
De communicatie moet wel goed overdacht zijn. Zo werd een van de medewerkers van TV5 Monde voor een interview naar aanleiding van de hiervoor genoemde hack gefilmd in zijn kantoor. Al snel ging er echter meer aandacht uit naar de wand achter hem dan naar wat hij te vertellen had: op de wand hingen namelijk diverse A4-tjes met wachtwoorden voor social media accounts van het tv-station… <<

Kim Gunnink werkt bij De Nederlandsche Bank en verdiept zich als beleidsmedewerker in cyberdreigingen ten aanzien van de financiële sector en het betalingsverkeer.